Installer Knoppix à partir d'un cédérom pour la récupération après sinistre

Gazette Linux n°114 — Mai 2005

Edgar Howell

Article paru dans le n°114 de la Gazette Linux de mai 2005.
Traduction française par Deny <deny CHEZ monaco POINT net>.
Relecture de la traduction française par Joëlle Cornavin <jcornavi CHEZ club TIRET internet POINT fr>.

Table des matières

1. Introduction

Un ami m'a récemment envoyé un céderom avec une version de Knoppix (http://www.knopper.net/knoppix/index-en.html) conçue pour pouvoir naviguer sans risque sur l'Internet. Bien que son seul but vaille la peine qu'on s'y arrête, ce qui m'a réellement bluffé est son utilisation pour restaurer un système endommagé.

Par un heureux hasard, je commençais juste à l'essayer un peu, quand notre neveu téléphona : « Écran bleu de la Mort ». Pas de sauvegarde. Je lui dis de passer le lendemain après-midi pour voir ce que pourrais faire. Windows ? ! Bien...

Pas de sauvegarde... Cette machine à été assemblée par des personnes qui savent vraiment ce qu'elles font. Leur façon d'employer les liens symboliques était un trait de génie.

2. Qu'est-ce que Knoppix ?

Knoppix est une mini-version autonome de Linux sur cédérom. J'en ai entendu parler, bien sûr, mais je n'ai jamais eu le temps de l'étudier plus avant. Grossière erreur. L'apprivoiser se révèle être d'un grand secours.

Cette version particulière est principalement destinée à transformer votre PC en une sorte de poste de travail sans disque dur. Après avoir amorcé sur le cédérom, un environnement analogue à un environnement sécurisé chroot est mis en place, sans accès à un quelconque disque dur. Vous pouvez y naviguer avec Firefox et même enregistrer les réglages, sur une disquette ou un support USB. Puis, quand tout est terminé, ce que vous n'avez pas enregistré vous-même explicitement quelque part réside dans l'historique.

Pas de virus. Pas de cheval de Troie. Pas de logiciel espion. Pas de cookies. Rien.

Il convient de noter que Knoppix (http://www.knopper.net/knoppix/index-en.html) m'a été recommandé par un ami qui n'avait aucune expérience antérieure de GNU/Linux, du fait que les logiciels qu'il utilise professionnellement ne sont disponibles que sous Windows. Mais il s'en sert maintenant pour accéder à Internet. Assez facile à comprendre. J'apprécie Firefox également.

3. Knoppix en action

J'admets volontiers ne l'avoir pas encore utilisé pour surfer. Néanmoins, c'est réellement un outil de restauration puissant ! Tom's Boot Disk (http://www.toms.net/rb/), qui se trouve sur le Ultimate Boot CD (http://www.ultimatebootcd.com/) a également toute mon estime, ainsi que quelques autres outils utiles. Mais vous devez expérimenter ses possibilités.

Peut-être faut-il préciser que Knoppix (http://www.knopper.net/knoppix/index-en.html) est basé sur Debian et que son noyau 2.4.29. date un peu. Mais il n'y a guère d'exploits possibles s'il n'y a nul endroit pour stocker des données. Et rien d'insolite à y regarder de plus près.

Une fois que vous avez amorcé, une interface graphique apparaît — en tant qu'utilisateur et non *root* — sous X11, dotée de toutes les fonctions nécessaires pour surfer. Voilà ! Pas de disque dur. Tout ce dont vous avez besoin pour accéder à l'Internet et rien de plus.

Cependant — il s'agit quoi qu'il en soit de Linux — il y a les autres terminaux virtuels. Tous préalablement authentifiés en tant que *root*.

J'ai pu très rapidement assembler un script simple avec lequel établir une connexion réseau. Le montage d'un lecteur ou d'une partition n'est pas plus difficile — Knoppix (http://www.knopper.net/knoppix/index-en.html) a déjà un fichier `/etc/fstab` configuré pour nous, avec les points de montage pour chaque partition unique formatée.

Les seules applications qui m'ont manquées pendant le temps où je l'ai utilisé sont Midnight Commander et netcat. Apparemment, netcat est entièrement autonome, car je n'ai eu aucun problème à le lancer après l'avoir recopié depuis une disquette, elle-même recopiée sur une Suse 8.0. La commande **cp -R** associée à netcat a dû remplacer mc à la volée (et sans SSH) au travers du réseau.

Knoppix semble s'accommoder assez bien du matériel éprouvé. Bien que X11 tournait sur mon Pentium® 166 avec 32 Mo de mémoire vive, je n'ai pas voulu me risquer à surfer. Et plusieurs interfaces avec des lignes de commande en tant que *root*, c'est le nirvana !

Je dois mentionner que je n'ai pas pu amorcer mon ordinateur portable Toshiba® (AMD K-5) de 5 ans depuis le cédérom. Il y a de nombreuses options que l'on peut saisir au démarrage, mais aucune ne m'a été utile. Je subodore quelque erreur avec un fichier nécessaire uniquement au portable — des erreurs de lecture répétées sur un bloc particulier. Il est notoire que les portables, étant de conception propriétaire, sont difficiles à configurer et à manipuler, ce n'est donc pas vraiment une surprise et rien de bien important pour moi.

4. Bidouiller « sous le capot »

Si l'on ne tient pas compte de son but initial, c'est un fabuleux outil pour la récupération après sinistre, offrant à la fois un réseau et des périphériques que l'on peut monter pour sauvegarder des données. Vous serez probablement encore amené à utiliser les outils que vous avez rassemblés au fur et à mesure, pour diagnostiquer des problèmes de matériel, par exemple. Et comme nous sommes *root*, nous devons toujours faire extrêmement attention à ce que nous faisons. Je n'ai eu aucun problème à me servir de fdisk pour reformater le second disque dur de notre neveu et allouer des partitions.

La façon dont les responsables du projet ont assemblé tout cela est vraiment impressionnante. Au lieu de tout câbler en dur, ils ont utilisé des liens symboliques avec talent. Après avoir remarqué que `/etc/hosts`, etc. sont des liens symboliques, j'ai en peu de temps écrit un script sur une disquette pour copier ce que je voulais faire dans `/tmp`, supprimer les liens et les remplacer par des références aux fichiers dans `/tmp`.

Tout ce qui était nécessaire pour configurer le réseau était de copier les fichiers `/etc/hosts`, `/etc/hosts.allow` et `/etc/hosts.deny` d'une machine vers le lecteur de disquettes, puis de mettre fin à la connexion pendant que notre neveu était là et son ordinateur relié au réseau. Pas d'approche à long terme, mais quelle efficacité dans la rapidité.

J'ai regardé le contenu de `/bin`, `/sbin`, `/usr/bin`, `/usr/sbin` et il semblerait que ce soit une distribution Linux assez complète : deux interpréteurs de commandes, lilo, divers mkfs*, awk, sed, ipchains, iptables, etc. Presque rien en matière de démons, gestionnaires de fenêtres ou fioritures, comme si quiconque s'en souciait dans l'environnement fourni. Comme ce cédérom n'est pas même à moitié rempli, vous pouvez vérifier si vos programmes favoris y figurent avant de créer le vôtre.

La version que j'ai reçue était une version en allemand, mais les textes des invites au démarrage étaient en anglais. Il devrait être assez simple de renommer deux fichiers pour passer à l'anglais avant de graver un cédérom. Cela pourrait également servir de modèle pour d'autres langues. Pure spéculation.

> L'image ISO de la Knoppix version 3.8.1-2005-04-08 (la dernière date du 5 mai 2005) contient presque 690 Mo — pas beaucoup d'espace pour des ajouts ! Reportez-vous à la mirrors page (http://www.knopper.net/knoppix-mirrors/index-en.html) pour télécharger la toute dernière version en plusieurs langues. — [dsrich]

Pour résumer, notre neveu a apporté son PC et nous l'avons connecté au réseau local. Grâce au réseau local et à une clé USB, nous avons pu récupérer environ 90% des données qu'il n'avait pas sauvegardées correctement à partir d'un lecteur apparemment sujet à une allergie à la chaleur propice à des erreurs de

lecture — ce lecteur contenait de plus un système d'exploitation ! Quand tout a été terminé, il était assez impressionné par ce que j'étais capable de faire.

Mais sûrement moins que je l'étais par Knoppix !

5. Post-scriptum

Si vous décidez de faire appel à ce logiciel pour accéder à Internet, soyez bien conscient de l'importance de ces sessions *root* — sans mot de passe ! Les seuls services disponibles sont l'imprimante et le moniteur. `/etc/hosts` et consorts sont étroitement verrouillés. Il faut toutefois noter que j'ai pu très facilement accéder au réseau.

Ainsi, si un quelconque individu malintentionné peut obtenir d'une façon ou d'une autre un accès frauduleux contre vous et l'exploite... C'est certainement une éventualité peu probable étant donné la cible — pas l'univers des PC, ni même GNU/Linux, juste une variété d'une version spécialisée de Linux. Mais donnez quand même à l'utilisateur *root* un mot de passe avant de graver votre propre copie.

Un livre qui traite de cela et d'autres utilisations de Knoppix est Knoppix à 200% (http://www.oreilly.fr/catalogue/2841773167.html) par Kyle Rankin — [dsrich].

Edgar est conseiller dans la région de Cologne et Bonn (Allemagne). Son travail quotidien consiste à assister ses clients pour établir la paie, à maintenir d'anciens programmes IBM® en assembleur, quelques autres en COBOL à l'occasion et autrement à utiliser QMF, PL/1 et DB/2 sous MVS.